Article

Common Law World Review

Common Law World Review
2020, Vol 49(3-4) 245–261

DOI: 10.1177/1473779520980556
journals.sagepub.com/home/clw

The Crypto-Wars myth: The reality of state access to encrypted communications

Cian C Murphy

Abstract

This article draws on four state studies to address a myth of the contemporary debate on internet communications: that, in the face of an internet 'going dark', states face a choice between absolute privacy and unfettered access to data. The legal powers which already exist suggest that certain states have a range of possible means of access to encrypted data. The lack of awareness over these powers may be because, despite public debate, democratic oversight remains deficient, while judiciaries and other institutions play useful but limited roles. The cross-territorial nature of the internet presents regulatory challenges and opportunities for reform—albeit in an environment in which the myth of Crypto-Wars is far from useful.

Keywords

encryption, surveillance, Crypto-Wars, lawful access, terrorism

The studies in this Symposium highlight the increase in tensions over the use of encryption since Edward Snowden's revelations about state surveillance. This has given rise to a new challenge for states: that the internet is 'going dark' or at least 'going spotty'. In this article, the lessons from the studies of Australia, Canada, New Zealand and the United Kingdom form the basis for a comparative analysis of instruments of lawful access. There are few existing studies in comparative counterterrorism law or policy which focus on the Five Eyes network.[1] Indeed,

1. One such study relates to 'closed material proceedings'. See David Jenkins, 'There and Back Again: The Strange Journey of Special Advocates and Comparative Law Methodology' (2011) 42(2) Colum Hum Rts L Rev 279.

University of Bristol, Bristol, UK

Author's note

This paper builds on the country studies of Australia (McGarrity and Hardy), Canada (West and Forcese), New Zealand (Keith) and the United Kingdom (Keenan) also published in 2020(3–4) *Common Law World Review*. These will be referred to as Author, text at n *, throughout this article.

Corresponding author:
Cian C Murphy, Reader in Law, University of Bristol, Bristol, BS8 1TH, Bristol, UK.
Email: c.murphy@bristol.ac.uk

researchers in journalism studies have argued that there is a lack of willingness on the part of both journalists and academics to investigate Five Eyes practices.[2] The comparative work that does exist is, by and large, done in policy and political studies rather than as comparative legal research. This is particularly the case in relation to state access to encrypted communications.

The 2015 report by the then UK Independent Reviewer of Terrorism Legislation, David Anderson QC, entitled *A Question of Trust*, summarises the Five Eyes states' laws on interception of communications in an extensive Annex.[3] The report also considers the challenge that encryption might pose for law enforcement. Encryption features, therefore, as a ceiling on the usefulness of interception powers. Anderson does not make specific proposals to address this matter, but one of his five principles is to 'minimise no-go areas' for law enforcement.[4] He concludes that 'there is a compelling public interest in being able to penetrate any channel of communication, however partially or sporadically'.[5]

A 2016 US Law Library of Congress paper examines the law on government access to encrypted communications in 12 states and the European Union (EU); 5 of which states were, at that time, EU members. Australia, Canada and the United Kingdom were included. The 'comparative summary' concludes that 'while there is a range of approaches among the surveyed countries, a majority make provision for specified intelligence or law enforcement agencies to obtain access to encrypted communications or the means of decryption under certain circumstances'.[6] The country reports, however, are brief and often omit any discussion of the use of available powers. The complexities of the law-in-practice which the authors highlight in this Symposium make clear that such an omission is significant. The Law Library's paper does, at least, confirm that access powers exist.

Work on encryption laws has also been done by the Carnegie Endowment's Encryption Working Group[7] and by the European Council on Foreign Relations.[8] The principal focus is on the EU and, to a lesser extent, the United States. This work also relates to policy and, although it aims to 'move the debate forward', it does not offer a clear analysis of existing laws or legal practice in key states. Thus, despite some excellent policy work, there is a clear need for doctrinal and contextual legal analyses that set out the powers which already exist in relation to lawful access.

The four country studies in this Symposium are part of that work and the analysis in this article relies heavily on those country studies. It also benefits from existing studies on the

---

Andrew Lynch, 'Control Orders in Australia: A Further Case Study of the Migration of British Counter-Terrorism Law' (2008) 8(2) OUCLJ 159.

2. Felicity Ruby, Gerard Goggin and John Keane, '"Comparative Silence" Still?' (2017) 5(3) *Digital Journalism* 353–67.
3. David Anderson QC, *A Question of Trust: The Report of the Investigatory Powers Review* (TSO, London 2015), Appendix 15: The Law of the Five Eyes.
4. Ibid [13.7].
5. Ibid [13.13].
6. Luis Acosta, 'Comparative Summary' in *Government Access to Encrypted Communications* (The Law Library of Congress, Washington DC 2016) 1.
7. For an overview of the work, see Encryption Working Group, *Moving the Encryption Policy Conversation Forward* (Carnegie Endowment for International Peace, Washington DC 2019).
8. Stefan Soesanto, 'No Middle Ground: Moving On From the Crypto Wars' European Council on Foreign Relations Policy Brief July 2018.

United States—in particular Kerr and Schneier's work on 'encryption workarounds'. Their 2018 *Georgetown Law Journal* study concludes:

> First, encryption workarounds are inherently probabilistic. None work every time, and none can be categorically ruled out. Second, the different resources required for different workarounds will have significant distributional effects on law enforcement. Some agencies will focus their efforts on a narrow set of workarounds and others will have broader options. Third, the scope of legal authority to compel third-party assistance will be a continuing challenge. And fourth, the law regarding encryption workarounds remains uncertain and underdeveloped.[9]

This Symposium illustrates that states already have legal powers which do—or at least could—provide access to encrypted communications. The first part of this article considers those powers in a fourfold typology. Second, the article demonstrates that oversight of the powers remains weak—hamstrung by political dynamics which afford much scope to the state in this field. Scandals have prompted law reform and there is increasing acknowledgement that judicial authorisation of warrants is central to the rule of law. However, parliamentary scrutiny remains deficient—in part because of secrecy and, perhaps, the challenge of technological literacy. Third, the article presents territoriality as the source of legal and operational problems—and also as a potential constraint on state overreach. The limits of state jurisdictions, multinational corporations as service providers, and the potential for transnational consumer and regulatory responses can all play a role in restraint of state power. The article concludes that it is necessary to dispel the Crypto-Wars myth of an impossible choice between absolute privacy and unfettered state access, to ensure that real progress is made towards rule of law safeguards and democratic oversight.

'Lawful access' in law and practice

Concerns about the internet 'going dark' or at least 'going spotty' are undoubtedly real. However, states already have legal powers to enable access to encrypted communications. Some such powers may already be in use. These powers are a subset of much broader state surveillance powers. That there is a lack of information, in particular about the use of powers, is not surprising. Surveillance powers have not always had clear legal bases or been subject to tight regulation. Often it is a public scandal, or litigation, which prompts regulation or reform.[10] The UK Investigatory Powers Act 2016 ('IPA'), for example, is a response both to the Snowden revelations and to litigation before national and European courts. Its enactment was done after three distinct reviews of the legislative framework.[11] It is Australia, however, which emerges from this Symposium as having the most extensive experience with decryption powers. Recent legislation in that jurisdiction raises the prospect of fines for service providers who do not assist

9. Orin S Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106 Geo LJ 989.
10. In the United Kingdom, this began with the case of *Malone v United Kingdom* [1984] 7 EHRR 14.
11. Anderson (n 3); Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework* (HC 1075, 12 March 2015); RUSI, *A Democratic License to Operate: Report of the Independent Surveillance Review* (July 2015). In addition to the three public reports, there was also a confidential report by Sir Nigel Scheinwald. That report relates to international cooperation, in particular with the United States, and how to regulate it. The report has not been published but a summary, which is in the public domain, sets out that matters on evidence exchange and cooperation would best be left to an instrument distinct to the IP Act. Sir Nigel Scheinwald, *Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing* (25 June 2015).

law enforcement and intelligence agencies with encryption.[12] In Canada, law enforcement authorities have had to adapt technology-neutral powers to use to access encrypted communications and have even resorted to dropping prosecutions when they would otherwise have to disclose their methods. The New Zealand approach, though 'cautious', nevertheless entails a power of interception which can require decryption. None of the four states, however, are entirely without legal instruments that could be used to access encrypted communications.

This article examines four types of such instruments. This work overlaps with a categorisation of 'workarounds' developed by Kerr and Schneier.[13] However, their classification was of operational approaches and not legal instruments per se. In contrast, the four types here are all instruments of law—warrants, notices and other powers:

(i) warrants to intercept communications;
(ii) 'technical capabilities notices' (TCNs) to request or require access;
(iii) warrants for 'equipment interference' or 'computer network exploitation';
(iv) powers of compulsion to require individuals or service providers to surrender access to a device.

One of the Kerr and Schneier workarounds (compel the key) does map onto one power (compelled disclosure). Another two workarounds (exploit a system flaw and access the data in plaintext) are encapsulated by a single power (equipment interference). The remainder—guess the key, find the key or locate the plaintext—are operational practices that do not necessarily entail specific legal instruments. As a typology of legal powers, the focus here is on the mechanism in law rather than the technology itself. Of course, the usefulness of any legal instrument, its oversight and authorisation and the implications for human rights will in part, however, depend on that technological aspect. Furthermore, as Kerr and Schneier conclude, no single power will yield access to all encrypted data.[14] A 'substitution effect' may occur in a state if legal safeguards make a previous law or policy less useful and the state turns to a new power.[15] There may also be an 'escalation effect' if service provider or user behaviour causes the state to have to choose a different power. However, notwithstanding the substitution or escalation effects, states do have powers of access. Whether or not these powers are in use remains unclear—a lack of transparency that, in some cases, is very much by design.

Warrants to intercept communications

The first legal instrument is a warrant to intercept communications. Interception warrants are available in all four states in this Symposium.[16] However, the interception of communications does not necessarily address encryption and the legal power to intercept communications has led to a reaction by users and service providers to secure their privacy. This is the 'going dark'

12. See McGarrity and Hardy, and the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth).
13. Kerr and Schneier (n 9).
14. Ibid.
15. Kent Roach, "Comparative Counter-terrorism Law Comes of Age" in Kent Roach, ed, *Comparative Counter-terrorism Law* (2015, Cambridge, Cambridge University Press), pp 11–12.
16. Telecommunications (Interception and Access) Act 1979 (Cth) (Australia); Protection of Privacy Act 1974 & CSIS Act 1984 (Canada); Telecommunications (Interception Capability and Security) Act 2013 (New Zealand); Investigatory Powers Act 2016 (UK).

or 'going spotty' phenomenon whereby the use of encryption makes intercepted material wholly or partially unreadable. West and Forcese highlight that, in Canada in 2018, approximately 70% of intercepted communications are encrypted. In Australia, McGarrity and Hardy report, the proportion of intercepted communications that are encrypted may be as high as 90%. This is the escalation effect in practice. Two types of service provider can be considered. The first is internet service providers ('ISPs'), sometimes termed communications service providers (CSPs), which give a user access to the internet via their network. The second is 'over the top providers' ('OTTs') who offer communication services—such as WhatsApp—via the internet. Both ISPs and OTTs might provide encryption and, if both do, render the task of getting intelligible intercept material even more difficult. New Zealand law is perhaps the most extensive in this type of power because it provides for access from ISPs that can, in principle, include the removal of encryption.[17] This power has its limits, for example, where the encryption is provided by an OTT, and the legislation recognises this limit.

The interception power in all states could be extended to also require that the data are provided in an intelligible format. The requirement would, in effect, necessitate the removal by the ISP of any encryption that the ISP itself provides. However, it would not overcome the challenge of OTT encryption. To overcome OTT encryption, two writers who work for GCHQ advocate a 'ghost protocol', which would make GCHQ a secret recipient of each message.[18] A coalition of over 50 civil society groups, companies (including Apple and Microsoft) and encryption experts rejected the proposal.[19] The technological implications would include the addition of a built-in vulnerability in the system that could become a target for malicious actors. There might also be a negative impact on user trust. Furthermore, the success of such an approach would itself be vulnerable to more sophisticated actors who could use additional encryption before they send data over the network. The prospect of forcible decryption of interception material also raises the first (but not the last) territoriality challenge. Whereas an ISP will likely be established within any jurisdiction in which it is a service provider, the same is not the case for an OTT. It would likely remain difficult to enforce a decryption order against an OTT which did not have a bricks-and-mortar presence in jurisdiction—a question to which the analysis returns.

Notices to request or require technical capabilities

A second type of legal instrument can request or require ISP or OTT companies to develop 'technical capabilities' to decrypt communications. The distinction between such an instrument and an interception warrant is one of technological and legal kind, and breadth. An interception warrant could mandate access to a particular user's communications data (and might necessitate changes to ISP or OTT systems to provide such data). A TCN can require system changes to a service provider's infrastructure and could, in principle, mandate direct access for law enforcement or intelligence agencies. This is broader in technological terms. It is also broader in legal terms. Each individual interception warrant requires authorisation by the state and compliance by the service provider. It is also more likely to target a single individual (though

17. Telecommunications (Interception Capability and Security) Act 2013 (New Zealand). Intelligence and Security Act ss 67(1) and 68(1). See Keith, this symposium, text accompanying fn 78.
18. Ian Levy and Crispin Robinson, 'Principles for a More Informed Exceptional Access Debate' *Lawfare* (29 November 2018).
19. 'Apple and WhatsApp Condemn GCHQ Plans to Eavesdrop on Encrypted Chats' *The Guardian* (30 May 2019).

note the use of bulk warrants). In contrast, a single authorisation for use of a technical capabilities power could allow access to data from all users of a particular service.

A TCN is, therefore, a legal instrument that is closest to the Clipper Chip of the 1990s. That was a microchip that the NSA sought to have included in communications devices to allow it to eavesdrop on users.[20] TCNs, as legal instruments, could be used to mandate the inclusion of a (software-based) Clipper Chip solution—and indeed go further—because the service provider themselves could be required to generate the solution. The need for safeguards is therefore, if anything, greater for TCNs than it is for interception powers.

Both the United Kingdom and Australia have TCNs while an analogous, albeit much more limited, power exists under Canadian law. The UK power is now found in the IPA.[21] Little attention was paid to this instrument during the UK legislative process. Nevertheless, its potency has become clearer in the time since. Draft regulations for the United Kingdom leaked in May 2017. They made clear that the Government sought to be able to use TCNs to force service providers to remove end-to-end encryption and ensure Government access to data.[22] In Australia, there is a three-tier approach to such notices. The first tier consists of Technical Assistance Requests (TARs), the second is Technical Assistance Notices (TANs) and the third is TCNs. Whereas TARs are voluntary, TANs and TCNs are compulsory.[23] In Canada, in contrast, the closest power which exists is that of the Solicitor General to issue Enforcement Standards for Lawful Interception of Telecommunications. As West and Forcese illustrate, these standards are not public. They also only relate to mobile telephone service providers. They do not, therefore, offer a means to regulate CSPs that offer home services, or OTTs.[24] The power is much more limited than the TCNs which exist in Australia and the United Kingdom. There is no such power in New Zealand law—though note that the New Zealand powers of interception appear broader than those in the other states.

One possible use of a TCN might be to require ISPs or OTTs to implement Levy and Robinson's ghost protocol proposal. The fact that TCNs remain secret means that such a power may already be in use. This secrecy is a key challenge to scrutiny and points to the limits of democratic oversight when legislation affords the Executive broad powers to create and implement rules. There is scope, in the United Kingdom, for the target of a TCN to seek review. However, the target is required to keep the TCN itself secret.[25] In Australia, individual employees face imprisonment if they fail to comply with secrecy requirements.[26] TCNs are a tool to covertly install a systemic vulnerability in services which, used to its full extent, could render all other instruments redundant.

Equipment interference or lawful hacking

In the course of the legislative process for the IPA, the UK Government, for the first time, avowed the use of 'equipment interference' by state agents.[27] In plain language, this is hacking

20. Steven Levy, 'Battle of the Clipper Chip' *New York Times* (12 June 1994).
21. See Keenan, text at n 40.
22. BBC News, Investigatory Powers: 'Real-time surveillance' in draft update, 5 May 2017.
23. McGarrity and Hardy, text at n 74.
24. West and Forcese, text at n 54.
25. IPA s 257(1), Keenan, text at n 52.
26. Telecommunications Act 1997 (Cth) s 317ZF, McGarrity and Hardy, text at n 79.
27. Owen Bowcott, 'GCHQ Accused of "Persistent" Illegal Hacking at Security Tribunal' *The Guardian* (1 December 2015).

done in the name of national security and crime control. Because it can, for example, provide access to a communications device while it is in use, state hacking can be useful where there is user-applied encryption that cannot be overcome by either the ISP or the OTT. State hacking can take a number of forms.[28] A state may choose to carry out equipment interference itself (either while a device is in use or after seizure of a device). It might also request access from manufacturers—such as the RCMP 2015 request to RiM to access a BlackBerry or the FBI's 2016 request to Apple. Alternatively, the state might acquire the means to hack a device from a third party. This is how the FBI ultimately did access Syed Farouk's iPhone data when Apple refused to assist it.

In the United Kingdom, equipment interference can only be undertaken by the intelligence and security services—not by law enforcement. The power must be used in a 'targeted' fashion within the jurisdiction but can be subject to a bulk warrant if it is being used overseas. The prospect of 'bulk' EI being used overseas was controversial, but Parliament was assured its use would be rare. In 2020, the Minister of State for Security and Economic Crime, Ben Wallace MP, wrote to the chair of the Intelligence and Security Committee (ISC) to inform him that it would be necessary to use the power more frequently.[29] This illustrates the risk that powers given under one set of circumstances may be used more broadly.

A similar power exists in Canada. However, criminal evidence disclosure rules in Canada mean that any lawful hacking risks being a 'one time only' tool. The disclosure of evidence gotten this way will alert malicious actors about the state capacity and give them the opportunity to adjust their behaviour.[30] In Australia, warrants for data surveillance include the use of programmes that can monitor data input and output.[31] Further, the Australian Security Intelligence Organisation ('ASIO') may apply for warrants for computer access. A wide definition of 'computer' means that an entire network may be exploited by such an instrument. The power allows ASIO to add, copy, delete or alter data in the course of the operation.[32]

The challenges of hacking by the state include the danger of the introduction of vulnerabilities into a user's (or service provider's) system which might be used by malicious actors to cause further harm. They also include the now-familiar concerns with secrecy and the challenges of oversight.

Compelled disclosure

The final legal instrument compels a user to disclose either the data sought by the state or the encryption key which guards the data. This can be done in the United Kingdom under s 49 RIPA or, in much wider circumstances, at ports and airports under sch 7 to the Terrorism Act 2000. Jonathan Hall QC, Independent Reviewer of Terrorism Legislation, has called for it to be an offence to refuse to decrypt a device in a counterterrorism investigation.[33] This offence would reduce the requirements that attach to a similar, existing, offence. It would replicate,

28. West and Forcese, text at n 81.
29. Letter from the Security Minister to Dominic Grieve QC MP to the Intelligence and Security Committee, 3 December 2018.
30. West and Forcese, text at n 89.
31. Surveillance Devices Act 2004, McGarrity and Hardy, text at n 46.
32. Australian Security Intelligence Organisation Act 1979 s 25A, McGarrity and Hardy, text at n 60.
33. Jonathan Hall QC, 'Scanning the Horizon: Technology and Risk' (Speech to the Henry Jackson Society, 22 January 2020).

away from ports, the extraordinary powers which exist under Terrorism Act 2000 at ports—at least in the context of a counterterrorism investigation.

The principal means of compulsion is criminal liability for refusal to comply. In New Zealand, the Search and Surveillance Act 2012 can require those subject to search to provide decryption passwords or other keys. Specific regime for border searches by customs officers also exists.[34] Canada, in contrast, does not have any law in place to compel disclosure. The most recent effort to develop such a power, in 2017, ultimately failed to do so.

This power has clear limitations. First, if the data on the device would incriminate the device-holder to a greater extent than the offence, then they are unlikely to comply. Second, if the power is used to compel a system, then they will immediately become aware of access, which places limits on the operational usefulness of the information. For example, it could not be the basis for a covert operation. Third, it may engage an individual's right not to incriminate themselves. Therefore, while this instrument has the least implications for service providers, it doesn't work where an individual refuses, something they are perhaps more likely to do if there are data which would benefit law enforcement or intelligence and security agencies.

Challenges for the rule of law

The country studies in this Symposium offer insight into how powers are drafted for technologies that change over time. Canadian law enforcement relies on largely 'tech-neutral' legal powers—some of which are decades old. In contrast, the UK's IPA is laden with provisions specific to particular technologies (eg the 'internet connection record'). With its focus on state activities in relation to matters where there may be an 'expectation of privacy', the Canadian regime is, arguably, more rights-focused and more future-proof. However, reliance on dated legal provisions was, in part, what led the UK to fall foul of European human rights law. The use of legal authorities from the 1980s might have complied in a bare-bones sense with the rule of law it did not meet European standards.[35] Thus, what is 'tech-neutral' in some eyes may be an unlawful extension of a legal authority in others. The challenge in this area of law is to achieve a satisfactory balance between powers that are broad enough to stay pace with shifts in technology, but narrow enough that their existence and use is foreseeable to the public, and to those responsible for oversight.

Secrecy is a further problem. In 2015, David Anderson QC was able to inform the UK Parliament and the public that all powers of which he was aware as Independent Reviewer had been made public. However, the existence of broad powers, such as to issue TCNs in secret, undermines the boost to public trust which an open and democratic process can provide. A power which can be secretly used to introduce systemic vulnerabilities that go far beyond other narrower and more explicit instruments vitiates that trust entirely. There is no guarantee that, for example, a TCN in the United Kingdom, or in Australia, does not already allow private—even encrypted—communications to be seen by states. This, the challenges of accountability take on further complexity when ISPs and—in particular—OTTs are transnational corporations. The question of territoriality will be the subject of further discussion. For now, it is sufficient to note that none of the four states under examination have been able to

34. Keith, text at n 83.
35. Liberty v. GCHQ [2015] UKIPTrib 13_77-H.

overcome the inherent territorial limits of the regulatory power. It may be impossible for them to do so on their own.

The Australian Independent National Security Law Monitor (INSLM), James Renwick, has explicitly endorsed several of the Anderson principles from *A Question of Trust*: the elimination of 'no-go areas' for law enforcement, the need for clarity about what the law permits and the need for oversight and safeguards.[36] Some means to access encrypted communications under some circumstances is already possible. This exposes the Crypto-Wars myth—in their arguments for further powers, law enforcement and intelligence agencies obscure the full extent of existing powers. A furious debate over the expansion of those powers may impede a rigorous debate about the (lack of) clarity of existing instruments and their use, and the effectiveness or otherwise of systems of oversight. It is to this question that the analysis now turns.

Rights, oversight and accountability

If there really are no no-go areas, then robust systems of authorisation, oversight and accountability are paramount to protect human rights. The powers available to facilitate state access to communications engage, and may violate, several rights. These include the right to privacy, the right to freedom of expression (including the right to receive information), the right to freedom of thought, conscience and religion, the right to freedom of association and the right against self-incrimination. Of course, the engagement of a right, and its infringement by the existence or use of a surveillance power, does not necessarily amount to a violation of that right. However, the infringement of rights does require justification to be legal. In general, it should have a clear legal basis, pursue a legitimate aim and be proportionate to that aim.

The manifestation of these rights in law differs across the four states. Canada and New Zealand have national bills of rights. The United Kingdom does not, though domestic implementation of European human rights law acts as a de facto national charter. Australia is the outlier—it has no national bill of rights whatsoever. A common baseline is the International Covenant on Civil and Political Rights (ICCPR), to which all four states are signatories, but which lacks the enforcement mechanisms of, for example, the European system.[37] EU standards play a significant role within that jurisdiction and outside of it. Those standards remain relevant in the United Kingdom (subject to Brexit) and also to New Zealand (which values its EU data protection 'adequacy' status). Alongside the ICCPR, and EU standards, there is a growing focus across the United Nations (UN) on *digital* privacy as a right in itself. The UN Special Rapporteur on the Right to Privacy is an example of a global office established in the aftermath of the Snowden revelations.[38] The Special Rapporteur on the Right to Freedom of Expression has also taken an interest in encryption and its implications.[39]

Three aspects of oversight and accountability merit attention: democratic oversight by legislatures; judicial authorisation of warrants and judicial review of laws and their uses; and the role of hybrid institutions. The key point here is that shortcomings across these three aspects

36. INSLM, 'What Are the Right Encryption Laws for Australia?' *Lowry Institute, Sydney* (5 March 2020).
37. International Covenant on Civil and Political Rights, New York, 16 December 1966.
38. UN Special Rapporteur Joseph Cannataci was appointed pursuant to UN Human Rights Council resolution 28/16. His latest annual report is available as of 27 July 2020 as UN Doc A/75/147.
39. See 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc A/HRC/29/32.

of oversight and accountability are a significant concern. They should give caution not only in relation to existing powers but also to any proposals for expansion of those powers.

Democratic oversight by legislatures

The legislature may have several relevant roles. First and foremost, if powers are to have a lawful basis, then it is the legislature that will ordinarily provide this basis.[40] In formal terms, the legislature enacts the law and therefore has the power to decide which of the above four types of instrument are available to the state. That formal position, of course, obscures the reality that in the Westminster model, a Government with a strong majority may be confident of its Bills becoming law. In such a case, then, the legislature's pre-legislative scrutiny should nevertheless test the Government's justifications for a law, consider its efficacy (and improve the law if it is not likely to be efficacious) and promote safeguards on state power.

The studies in this Symposium illustrate a variety of legislative histories and parliamentary behaviours. Australia has the greatest number of Acts of Parliament on terrorism of any of the four states—a result of fervent lawmaking over the past 20 years. The UK's IPA may be the single most extensive statute in this policy field. In contrast, the Canadian Government seems reluctant to grab the legislative bull by the horns, despite occasional attempts to do so. In the event that the political will to act shifts, for example as a result of a serious crime or violent attack, there are provisions ready for the statute books. New Zealand, the outlier in this Symposium, has taken a more cautious approach.

Keith attributes that caution, in part, to the tendency towards coalition in the New Zealand political system. The same occurred in the United Kingdom in 2010–2015 when the Conservative Party was in coalition with the Liberal Democrats (the first coalition in the United Kingdom since World War II). It was the Liberal Democrat's refusal to support the Communications Data Bill in 2012 which stopped it from becoming law. Outside that period, both Labour and Conservative Party governments have promoted surveillance powers. As a policy field it is, like counterterrorism law, 'bi-partisan'.[41] In Canada, in contrast, West and Forcese describe the subject as 'consistently toxic' for successive governments.[42]

Even where the passage of a Bill into law is assured, the process itself remains an opportunity for scrutiny. Anderson notes that the legislative process which led to the IPA saw extensive scrutiny—which began with the three reports from Anderson himself, Parliament's ISC, and Royal United Services Institute.[43] On the other hand, the sheer extent of the Act meant that as a Bill there was too little time to adequately scrutinise all provisions, such as those relating to TCNs. Such laws' increasing technical complexity, alongside legal complexity, and the dictates of secrecy make pre-legislative scrutiny difficult—perhaps impossible.[44]

40. I set aside here the prospect of prerogative powers being used in this field.
41. Lydia Morgan and Fiona de Londras, 'Is there a "Conservative" Counter-Terrorism?' (2018) 29(2) KLJ 187.
42. West and Forcese, text at n 28.
43. David Anderson QC, 'The Investigatory Powers Act 2016—An Exercise in Democracy' (3 December 2016) <https://www.daqc.co.uk/2016/12/03/the-investigatory-powers-act-2016-an-exercise-in-democracy/> accessed 1 November 2020.
44. See for some examples Graham Smith, 'The Investigatory Powers Act 2016—Swan or Turkey?' (31 December 2016). See further Cian C Murphy, 'State Surveillance and Social Democracy' in Alan Bogg, Jacob Rowbottom and Alison Young (eds), *The Constitution of Social Democracy* (Hart Publishing, Oxford 2020).

The second side of the legislature's role is post-legislative scrutiny. The authors in this Symposium draw attention to the roles of the Parliamentary Joint Committee on Intelligence and Security (Australia), the Standing Committee on Public Safety and National Security (Canada), the ISC (New Zealand) and the Parliamentary Joint Committee on Intelligence and Security (United Kingdom). However, there are far more references to, and much more extensive discussion of, non-parliamentary mechanisms of oversight—such as Independent Reviewers, an Inspector-General and Royal Commissions.

It would be too great a leap to suggest that this alone indicates the lesser significance of parliamentary scrutiny. However, McGarrity and Hardy, for example, do point to the significant limitations of the Australian committee, which cannot examine operational matters. Keith briefly mentions the New Zealand committee, which is subject to the same limitation, though it can request that the Inspector-General of Intelligence and Security conduct an investigation.[45] Goldman identifies two facts that limit the US Congress' role in effective intelligence oversight—the fragmentation of responsibility between different Congressional committees, and the asymmetry of information between the Executive and Congress in this area.[46] These limitations, at least on the evidence available in this Symposium, are not limited to the US legislature but also play a part elsewhere. They will require attention if legislatures are to fulfil their oversight function—one that ought to be central to their broader role as a site of democratic consent to surveillance.

Judicial authorisations and judicial review

The judicial function is of increasing significance and two aspects merit scrutiny here: prior authorisation of warrants and post hoc review of laws and operations.[47] In the lead-up to the adoption of the IPA, a particular point of debate was whether judges or Ministers should authorise warrants for the various powers in the law. The judiciary offer expertise in the law and independence of the Executive. Ministerial authorisation, in contrast, largely draws its claim to legitimacy from the Minister's accountability for security. The Independent Reviewer, drawing comparisons to other warrants, opted for judges. The ISC's recommendation was for Ministerial authorisation. RUSI recommended that both institutions play a role—and it was this perspective that won out.[48]

Judicial authorisation is necessary in Australia for interception warrants—with applications made to a judge, magistrate or appropriate member of the Administrative Appeals Tribunal.[49] The exception is the ASIO, whose warrant applications are considered by the Commonwealth Attorney-General.[50] In Canada, interception almost always requires judicial authorisation,[51]

45. Keith, text at n 88.
46. See Zackary K Goldman, 'The Emergence of Intelligence Governance' in Zackary K Goldman and Samuel J Rascoff (eds), *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (OUP, Oxford 2016) 224.
47. The same two aspects are used by West and Forcese in Leah West and Craig Forcese, 'Judicial Supervision of Anti-Terrorism Laws in Comparative Democracies' in Ben Saul (ed), *Research Handbook on International Law and Terrorism* (2nd edn Edward Elgar Publishing, Cheltenham 2020).
48. See Anderson (n 3), Recommendation 22; Intelligence and Security Committee of Parliament (n 11) 73–76; RUSI (n 11) para 5.60.
49. TIA s 6DB, see McGarrity and Hardy, text at nn 16–20.
50. TIA s 9; see also McGarrity and Hardy, text at n 21.
51. West and Forcese, text at nn 37–39.

whereas in New Zealand there is also a form of 'double-lock' which requires authorisation from a Minister alongside a Commissioner of Intelligence Warrants.[52] There is therefore a trend towards judicial authorisation of warrants, up to a point. In the UK, for instance, aside from the Ministerial role, there is also the fact that the Judicial Commissioners, though judges, do not perform their authorisation function in a judicial capacity.[53] Although there is not the space here to consider it at length, a complete comparison of judicial authorisation would also include an examination of the applicable test. In Australia, for example, the bar is set low—it merely requires that information *likely* to be obtained would be *likely* to assist an investigation.[54] This appears rather a low hurdle to vault given the extent of the potential interference with rights.

The second aspect of the judicial function is that of judicial review of laws themselves and of their operation. This has been vital in the UK, for example, since, even before the *Malone v United Kingdom* decision, the European Court of Human Rights first got to grips with covert surveillance in *Klass v Germany*.[55] However, judicial review is a blunt tool to assess the overall impact of surveillance measures. The necessity of covert powers is difficult to substantiate without disclosure of operational matters. This contributes to a difficulty in assessment of proportionality. On the one side of the scale is the necessity of such powers, and of a particular use of those powers, and on the other side is an impact on human rights that is hard to perceive, at both an individual and a societal level. There may well be a chilling effect on online activity and, indeed, this may be an intended outcome of surveillance. There is a security gain if malicious individuals refrain from unlawful behaviour because of the existence or use of surveillance powers. However, there is a collateral impact on individuals who engage in lawful political activism.[56] It is difficult for a court which faces a particular challenge to particular powers to weigh all of these values. That they have had to do so is perhaps further evidence of the failure of legislatures to grapple with them.

Hybrid institutions: Transparency and trust

The field of counterterrorism law has given rise to several new 'hybrid' institutions which blur the lines between the executive and other branches of government.[57] The particular domain of surveillance powers exemplifies this trend. At their best, they can complement the traditional organs of government, improve operation and oversight and bolster public confidence. These goals—that there is appropriate oversight and that the oversight be transparent enough to ensure public trust—are in tension. A secret review mechanism may achieve the first but will struggle to achieve the second. Contrariwise, if the accountability mechanism is entirely transparent, then those institutions under scrutiny may become more hostile, if to be seen to change casts doubt on the legality or propriety of past activities. A balance must therefore be struck between the achievement of the two goals. Hybrid institutions can play a role in this

52. Keith, text at n 86.
53. IPA s 277(2) provides that 'A person is not to be appointed as the Investigatory Powers Commissioner or another Judicial Commissioner unless the person holds or has held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005)'.
54. TIA s 46.
55. *Malone v United Kingdom* (n 10); *Klass v Germany* (1979–1980) 2 EHRR 214.
56. Human Rights Watch, *Perils of Backdoor Encryption Mandates* (26 June 2017) <www.hrw.org/news/2017/06/26/perils-back-door-encryption-mandates> accessed 1 November 2020.
57. Paul F Scott, 'Hybrid Institutions in the National Security Constitution: The Case of the Commissioners' (2019) 39(3) LS 432.

work only if they, themselves, maintain a high level of public and political trust. In his valedictory review of the office of Independent Reviewer of Terrorism Legislation, David Anderson QC presents a more complex, and fluid, image of 'channels of influence' than the somewhat binary debate between whether it is the legislature or judiciary which can best hold the executive to account in this field.[58]

The bodies identified in this Symposium include that Independent Reviewer (UK) and the INSLM (Australia), the Inspector-General of Intelligence and Security (New Zealand), Commonwealth Ombudsman (Australia) and the Privacy Commissioner (Canada), among others. Research in counterterrorism law and operations increasingly focuses on such institutions and further study is necessary.[59] There remains the risk that such institutions become subject to capture—wherein to maintain trust and confidence within the state, and because of the secrecy with which they must operate, they lose—or are seen as losing—their independence.[60]

This survey of the institutional landscape paints a picture of an accountability framework being pushed to the limits. Legislatures are limited by the pressures of national security politics that militate in favour of the state. The judiciary's role is limited both because not all powers require judicial authorisation and because judicial review is not always the most appropriate forum for policy decisions. Hybrid institutions, meanwhile, must sail between Scylla and Charybdis to maintain the trust of the security agencies, sceptical publics and civil societies. It is against this backdrop of national institutions under stain that we turn to the impact of the inherent cross-territoriality of the internet.

Territoriality, enforcement and constraints

State access to encrypted communications is, by implication if not by strict definition, about state access to internet communications. The internet poses potent challenges for state regulation. Some service providers which states seek to regulate may not maintain a 'bricks-and-mortar' presence, or indeed any legal presence, in a jurisdiction—as West and Forcese illustrate by reference to Facebook's refusal to comply with a Canadian court order.[61] And on the other hand, if service providers do facilitate such requests, or comply in the converse example of the regulation of users outside a state's territory when the service provider does have a presence in that territory, then they run the risk of a conflict of laws. The traditional means to overcome such conflicts—Mutual Legal Assistance Treaties—are cumbersome. It is unsurprising, therefore, that states in this study have sought to give their laws some form of extraterritorial effect. However, as the Facebook example evidences, the efficacy of extraterritorial enforcement may end up as a matter of raw power as often as it is one of law. In addition to posing problems of effectiveness, extraterritorial exercises of powers can also present challenges for accountability and redress. In the United States, for example, there is a difference between

58. David Anderson QC, 'The Independent Review of Terrorism Laws' (2014) PL 403.
59. See, eg, Jessie Blackbourn, 'Independent Reviewers as Alternative: An Empirical Study from Australia and the United Kingdom' in Fiona de Londras and Fergal Davis (eds), *Critical Debates on Counter-Terrorism Judicial Review* (CUP, Cambridge 2014), and more recently Jessie Blackbourn, Fiona de Londras and Lydia Morgan, *Accountability and Review in the Counter-Terrorist State* (Policy Press, Bristol 2019).
60. Ibid 135–36.
61. West and Forcese, text at n 77.

constitutional protections for US citizens and those protections for non-citizens.[62] Even if there is not a difference in law, it may be difficult to effectively access accountability and redress mechanisms from outside a jurisdiction. A common fear among is that state agencies would engage in mutual 'off-shoring' of surveillance to escape oversight. As Der Spiegel puts it:

> And it appears that the principle that foreign intelligence agencies do not monitor the citizens of their own country, or that they only do so on the basis of individual court decisions, is obsolete in this world of globalized communication and surveillance. Britain's GCHQ intelligence agency can spy on anyone but British nationals, the NSA can conduct surveillance on anyone but Americans, and Germany's BND foreign intelligence agency can spy on anyone but Germans. That's how a matrix is created of boundless surveillance in which each partner aids in a division of roles.[63]

It is in this context, and in light of increasing public scrutiny, that states now seek to regulate. Because of the cross-territorial nature of the phenomenon, unilateral regulation in this field is unlikely to be successful, and yet cooperation remains difficult.

After the UK's departure from the EU, the Five Eyes represents an entirely distinct collection of states which may have sufficient regulatory power to shape the global debate on lawful access. Nevertheless, that regulatory power requires consensus to be effective. Neither Canadian nor New Zealand authorities joined a 2019 open letter from Australia, the United Kingdom and the United States to Facebook. The letter, in response to the company's intention to adopt platform-wide end-to-end encryption, called on Facebook to instead 'enable law enforcement to obtain lawful access to content in a readable and usable format'.[64] This is remarkable, not only because it may illustrate differences in Five Eyes policy positions but also because it is a letter which asks the company to act. It is not regulation. The last attempt to do so in the United States, a 2016 Bill sponsored by Senators Burr (Republican) and Feinstein (Democrat) failed, in part because of lack of support from the Obama administration.[65] The other four states, as this Symposium illustrates, do have powers to access encrypted material, and yet it seems likely that further regulation will be called for—if only to address the territoriality challenge.

If states are unable to regulate, then the decisions of private companies take on a greater role in governance. The potential for them to exercise discretion over their cooperation is significant. BlackBerry has refused to cooperate with demands by Pakistan for access but did give access to authorities in India and Saudi Arabia.[66] More powerful states have even greater influence over internet services in their territories.[67] In China, for example, encryption services may only be offered subject to a Government licence.[68] As the debate over encryption gains

62. David Cole, *Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism* (The New Press, New York 2003).
63. 'How the NSA Targets Germany and Europe' *Der Spiegel* (1 July 2013).
64. 'Open Letter: Facebook's "Privacy First" Proposals' (4 October 2019).
65. Electronic Frontier Foundation, 'Security Win: Burr-Feinstein Proposal Declared "Dead" for This Year' (27 May 2016).
66. 'BlackBerry bows to Saudi Arabia' *The Register* (9 August 2010); 'BlackBerry gives Indian Government Ability to Intercept Messages' *Wired* (11 July 2013); 'BlackBerry to Keep Operating in Pakistan' *BBC News* (31 December 2015).
67. For a discussion of how the internet may become more 'nationalised', see E Schmidt and J Cohen, *The New Digital Age: Reshaping the Future of Peoples, Nations, and Business* (John Murray, London 2013).
68. Y. Luo, E. Carlson, and Z. Yu, "China Enacts Encryption Law", Covington Inside Privacy, 31 October 2019.

momentum, transnational service providers face a choice: either to vary their services across jurisdictions or to become vectors for the diffusion of standards which more powerful regulators impose. This is being done at a time when some efforts at international cooperation exemplify what Ginsburg has called 'authoritarian international law' whereby States with common illiberal and anti-constitutional goals seek to deploy institutions and processes of international law to pursue those goals.[69]

The EU may be the likeliest source of new rules that cleave more towards democratic constitutional values. It has the institutional infrastructure—and perhaps the political will—to adopt such rules. A 2016 EU survey which received responses from 25 Member States and Europol found that 'encryption is encountered often or almost always in the context of criminal investigations'.[70] At that point, five Member States (Croatia, Italy, Latvia, Poland and Hungary) sought a law to force decryption.[71] However, in 2020, the EU is 'set to declare war on encryption'.[72] The headline is misleading. A leaked internal memorandum states that 'Potential technical solutions will have to enable authorities to use their investigative powers which are subject to proportionality, necessity and judicial oversight under their domestic legislation, while upholding fundamental rights and preserving the advantages of encryption'.[73] That EU counterterrorism law can be illiberal is not news.[74] But the prospect of EU legislation does not, of itself, spell the end for encryption or for online privacy.

If the EU does legislate, the implications will not stop at Europe's shores. EU standards, for example, may become global standards if companies regulate in accordance with EU rules to ensure market access and adopt uniform standards across the world for ease of service provision. This makes the EU a vital site for the development of laws which comply with the principles such as proportionality, necessity and judicial oversight, to which the EU document refers. If access to encrypted communications in the EU was only possible where certain safeguards are in place, then it would be easier for companies to resist the dictates of illiberal regimes elsewhere.

Regulation aside, some restraint may come both from service providers and from intelligence agencies themselves. Transnational corporations such as Apple, Microsoft and Facebook are among the most influential global entities in terms of impact on national law and international regulation. Examples include Apple's refusal to cooperate with the FBI in the *#ApplevFBI* controversy, Facebook's assertive position in relation to end-to-end encryption in WhatsApp and Messenger and the strong rebuff of the 'ghost protocol' proposal by these and other companies. Of course, these service providers are likely driven, at least in part, by consumer concerns, and therefore an active public debate remains vital. Deeks points to the

69. Tom Ginsburg, 'Authoritarian International Law?' (2020) 114(2) AJIL 221.
70. Council of the European Union, 'Encryption of Data: Mapping of the Problem—Orientation Debate' Doc 13434/16, Brussels, (21 October 2016) 3.
71. 'Five Member States Want EU-wide Laws on Encryption' *Euractiv.com* (22 November 2016). There are also proposals for a Regulation on Cross-Border Access to Evidence—see Sergei V Maymir, 'Anchoring the Need to Revise Cross-Border Access to E-evidence' (2020) 9(3) *Internet Policy Review*.
72. 'The EU is Set to Declare War on Encryption' *The New Statesman* (21 September 2020).
73. 'Draft Council Resolution on Encryption—Security through Encryption and Security Despite Encryption' *Brussels* (6 November 2020).
74. Cian C Murphy, *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* (Hart Publishing, Oxford 2012).

prospect of 'peer constraint' within the intelligence communities.[75] This is the idea that intelligence agencies will be sensitive to media scrutiny, leaks and public outcry and so will be cautious about their operations and their cooperation with other agencies. This may well help to shape their behaviour—but two other dynamics must also be borne in mind. The first is the security imperative to which they owe their existence and the second is that peer constraint itself relies on public awareness or at least the potential for public awareness. Both self-regulation and intelligence peer restraint are, therefore, dependent on the sorts of publicity that oversight mechanisms bring. The key for the future may lie in a creative tension in the government, industry and civil society as they negotiate their respective interests in the context of an increasingly privacy-conscious public.

Beyond the 'Crypto-Wars' myth

The idea of a 'Crypto-War' which pits absolute user privacy against unfettered state access to communications is a myth. For the average internet user, there is no absolute privacy on the internet. The basic connection data which ISPs collect, alongside cookie data held by ordinary websites, and myriad other records, make this a reality. However, users and service providers can and do use encryption to make their internet use more secure. This may leave the internet 'spottier' for those who look to surveil it—but it has hardly 'gone dark'. This is in part because several governments—Australia, Canada, New Zealand and the United Kingdom among them—have legal instruments which enable them to access internet communications.

The increase in use of encryption is an example of escalation—a response to reckless (and unlawful) behaviour by states in the past. That encryption means that, despite the powers which states now have, a digital panopticon might be a useful dystopia—but it is unlikely to become a reality. The fact that US authorities have not been able to access all data they have sought—*even with legal authority*—gives the lie to the idea that all that is needed is the right legal instruments.[76] If users are sophisticated, they will use a combination of ISP, OTT and third-party security measures to ensure that their communications are not readily readable. The significant costs of decryption mean that law enforcement authorities and intelligence agencies will only be able to deploy such tools in particular cases.

It is, of course, the case that there can be no backdoor 'only for the good guys'.[77] Any vulnerability in encryption may be exploited not only by state actors but also by malicious ones. One possible way to avoid this—used for example in the Netherlands where the government endorses encryption—is to rely more heavily on lawful hacking.[78] Lawful hacking, subject to prior judicial authorisation and appropriate political oversight, can avoid certain problems. It is more secure than the installation of systemic vulnerabilities that malicious actors might use to facilitate identity theft, fraud and other crimes. Because there is a capabilities gap, only some

75. Ashley Deeks, 'Intelligence Communities, Peer Constraints, and the Law' in Zachary K Goldman and Samuel J Rascoff (eds), *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (OUP, Oxford 2016).
76. Soesanto (n 8) 10–11. Note that Soesanto also reports scepticism in the *Washington Post* about the extent of the law enforcement problem—a dispute which further evidences the challenges of secrecy in the field.
77. INSLM (n 32) p 6.
78. NL Times, 'Dutch Parliament Approves Bill to Hack Criminal Suspects' (21 December 2016).

states will be able to undertake it. There remain challenges of oversight, of accountability for uses of the power and of redress for misuses, which may be even greater given the potency of equipment interference.

The point is not to advocate for state hacking. It is to argue that it is necessary to move past the myth that there is a binary choice. The existence of at least some decryption instruments in Australia, Canada, New Zealand and the UK suggests that the legal framework allows more than might be understood by the public or even politicians. The lack of clarity may in part be because states have made laws in response to scandals. Such circumstances can shine a light on the policy area but do not always lead to the most careful of lawmaking. If the EU's attempt to adopt new rules is successful, it will increase the pressure on the Five Eyes states to follow suit. If it does so, it will be against the backdrop of fractious and increasingly authoritarian global politics. In such a context, myths, however vivid, are best left to the storybooks.

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.